

Procédé de surveillance de messages destinés à l'initialisation de sessions d'échange de flux multimédias, serveur et installation mettant en œuvre ce procédé

La présente invention concerne un procédé de surveillance de messages destinés à l'initialisation de sessions d'échange de flux multimédias, un serveur et une installation mettant en œuvre ce procédé.

5 Plus précisément, l'invention concerne un procédé de surveillance de messages destinés à l'initialisation de sessions d'échange de flux multimédias transmis en mode paquets via un serveur de surveillance par un réseau entre un terminal émetteur et au moins un terminal récepteur.

On entend par initialisation le fait d'établir, de modifier ou de fermer une session au cours de laquelle des flux multimédias sont échangés.

10 Par la suite, nous décrirons l'invention en nous fondant sur le protocole SIP. L'invention n'est cependant pas limitée à ce seul protocole.

Le protocole SIP (Protocole d'Initialisation de Session) est un protocole de la couche Application du modèle OSI permettant l'établissement, la modification ou la fermeture d'une session au cours de laquelle des flux multimédias sont échangés entre  
15 un terminal émetteur et au moins un terminal récepteur.

Ce protocole SIP utilise des messages qui circulent sous forme de paquets dans un réseau SIP composé de serveurs de traitement spécifiques. Le réseau SIP est un réseau en recouvrement d'un réseau IP. Le chemin emprunté par les messages SIP n'est donc pas forcément le même que celui emprunté par les flux multimédias.

20 L'établissement de la session consiste à définir, grâce à l'échange de messages SIP, le type et le format des flux multimédias (par exemple les codecs utilisés) que les terminaux désirent se transmettre. En cours de session, des messages SIP peuvent être échangés entre les terminaux pour convenir d'un nouveau format des flux multimédias. Enfin, des messages SIP sont à nouveau échangés lors de la fermeture de  
25 la session.

Généralement, l'opérateur du réseau sur lequel sont échangés les flux multimédias facture l'utilisateur du terminal ayant établi la connexion, en fonction de la durée de la session d'échange de flux multimédias. Si le terminal n'arrive pas à établir la connexion malgré l'échange de messages SIP, l'opérateur ne facture pas l'utilisateur de  
30 ce terminal.

Or il est possible pour un utilisateur mal intentionné d'utiliser les messages SIP eux-mêmes ainsi que la bande passante allouée par l'opérateur pour leur

-2-

transmission, pour y inclure des données non liées à l'établissement d'une connexion, notamment les données multimédia elles-mêmes. En effet, l'opérateur ne vérifie pas en général le contenu des messages SIP.

L'utilisateur peut donc finalement échanger des informations multimédia sur le réseau sans que l'opérateur ne lui facture cet échange.

Pour remédier à cet inconvénient, on connaît déjà dans l'état de la technique, des procédés mis en œuvre par les serveurs de traitement SIP qui consistent à limiter la transmission de messages SIP aux messages contenant uniquement des éléments d'information prédéfinis, adaptés aux services que souhaite fournir l'opérateur du réseau à ses utilisateurs.

Ce procédé nécessite cependant une capacité de traitement importante au niveau des serveurs de traitement SIP qui comparent chaque message SIP aux messages autorisés par l'opérateur. Il nécessite de plus une mise à jour des serveurs de traitement SIP chaque fois que l'opérateur décide de modifier les types de messages SIP autorisés à transiter sur son réseau. Cette solution est efficace mais complexe et coûteuse à mettre en œuvre.

L'invention a pour but de remédier à ces inconvénients en fournissant un procédé de surveillance de messages destinés à l'initialisation de sessions d'échange de flux multimédias capable de vérifier que les messages d'initialisation de session ne sont pas utilisés pour transmettre de manière détournée de l'information, sans pour autant vérifier le contenu de chaque message d'initialisation transitant dans le réseau.

A cet effet, l'invention a pour objet un procédé de surveillance de messages destinés à l'initialisation de sessions d'échange de flux multimédias, ces messages étant transmis en mode paquets via un serveur de surveillance par un réseau entre un terminal émetteur et au moins un terminal récepteur, caractérisé en ce qu'il comporte les étapes suivantes :

- on estime une valeur de débit pour au moins un paquet d'initialisation reçu par le serveur de surveillance,
- on compare cette valeur à une valeur de débit maximal autorisé,
- on autorise la transmission du paquet d'initialisation uniquement si la valeur de débit pour ce paquet d'initialisation ne dépasse pas la valeur de débit maximal autorisé.

Grâce à la surveillance du débit des paquets SIP transitant dans le réseau, l'invention permet de détecter les paquets SIP détournés qui, contenant des informations inutiles au protocole SIP, augmentent de manière anormale leur propre débit. La transmission de ces paquets SIP est alors interrompue.

Un procédé de surveillance de messages transmis en mode paquets selon l'invention peut en outre comporter l'une ou plusieurs des caractéristiques suivantes :

- 5           – on définit pour chaque couple formé d'un terminal émetteur et d'un terminal récepteur, un canal de transmission, associé à une valeur de débit maximal autorisé spécifique ;
- 10          – l'estimation de la valeur de débit pour le paquet d'initialisation reçu par le serveur de surveillance comporte une étape au cours de laquelle on garde en mémoire les tailles des derniers paquets d'initialisation émis par le terminal émetteur à destination du terminal récepteur et reçus par le serveur de surveillance depuis une durée prédéterminée et une étape au cours de laquelle on divise la somme des tailles des paquets d'initialisation mémorisés par la durée prédéterminée ;
- 15          – le procédé est mis en œuvre par le serveur de surveillance, celui-ci étant en outre dédié au traitement des paquets d'initialisation de sessions ;
- 20          – on contraint l'acheminement des paquets d'initialisation de sessions vers le serveur de surveillance en tant que premier serveur de traitement traversé par ces paquets d'initialisation de sessions ;
- le serveur de surveillance étant l'un quelconque des serveurs de traitement des paquets d'initialisation de sessions, on définit des règles de routage assurant un transit systématique des paquets d'initialisation de sessions par ce serveur de traitement ; et
- les messages d'initialisation de sessions transmis utilisent le protocole SIP.

25          L'invention a également pour objet un serveur de surveillance de messages destinés à l'initialisation de sessions d'échange de flux multimédias, ces messages étant transmis en mode paquets via un serveur de surveillance par un réseau entre un terminal émetteur et au moins un terminal récepteur, caractérisé en ce qu'il comporte :

- 30           – des moyens d'estimation d'une valeur de débit pour au moins un paquet d'initialisation reçu par le serveur de surveillance,
- des moyens de comparaison de cette valeur à une valeur de débit maximal autorisé,
- des moyens d'autorisation de la transmission du paquet d'initialisation uniquement si la valeur de débit pour ce paquet ne dépasse pas la valeur de débit maximal autorisé.

-4-

L'invention a également pour objet une installation de transmission de messages destinés à l'initialisation de sessions d'échange de flux multimédias comportant un réseau et au moins un serveur de surveillance selon l'invention.

L'invention sera mieux comprise à la lecture de la description qui va suivre,  
5 donnée uniquement à titre d'exemple et faite en se référant aux dessins annexés dans lesquels :

- la figure 1 est un schéma représentant une installation pour la mise en œuvre d'un procédé selon l'invention,
- la figure 2 est un schéma fonctionnel représentant les étapes successives  
10 d'un procédé selon l'invention.

On a représenté sur la figure 1 un terminal émetteur 10 communiquant avec un terminal récepteur 12 par l'intermédiaire d'un réseau 18 de transmission de données.

Les terminaux 10 et 12 sont par exemple des ordinateurs ou des téléphones, et le réseau de transmission 18 de données est un réseau IP 18 ou un réseau  
15 téléphonique commuté en combinaison avec un réseau IP.

Le réseau 18 de transmission de données est constitué par un ensemble de routeurs 14, 16, reliés entre eux, dont la fonction est d'assurer un routage correct des messages entre les terminaux 10 et 12, au travers du réseau 18 de transmission de données.

20 Les terminaux 10 et 12 s'échangent à la fois des messages d'initialisation destinés à l'initialisation de sessions d'échange de flux multimédias et des flux multimédias. Nous considérerons dans la suite de la description que les messages d'initialisation sont des messages SIP.

Ces messages SIP sont transmis en mode paquet, c'est à dire qu'ils sont  
25 transmis sous forme d'une pluralité de paquets.

Le réseau 18 de transmission de données est également constitué par des serveurs 20, 22 de traitement des paquets SIP spécifiques, interconnectés sous-forme d'un réseau 24 en recouvrement du réseau de transmission 18 de données. Ce réseau 24 en recouvrement du réseau de transmission 18 est appelé réseau SIP 24 dans la suite de  
30 la description car il est dédié au transfert de messages SIP. La fonction des serveurs de traitement SIP 20, 22 est d'assurer le routage correct des paquets SIP entre les terminaux 10 et 12 au travers du réseau SIP 24.

Lorsque deux terminaux 10 et 12 souhaitent établir une connexion pour l'échange d'un flux multimédia 26, ils s'échangent un flux SIP 28 pour définir le type et le  
35 format de ce flux multimédia 26.

Ces deux flux suivent généralement des chemins réseaux différents. Le chemin suivi par les flux multimédias 26 dépend des adresses IP des ordinateurs 10, 12. Il est déterminé par les routeurs IP 14, 16 du réseau. Le chemin suivi par les flux SIP 28 peut dépendre des adresses IP des ordinateurs 10, 12, mais aussi des numéros de téléphone ou des adresses de messagerie des utilisateurs des ordinateurs 10, 12. Il est déterminé par les serveurs de traitement SIP 20, 22 et transite nécessairement par le réseau SIP 24.

Dans le réseau SIP 24, les flux SIP 28 sont transmis sur différents canaux SIP et sont identifiables à l'aide des adresses des ordinateurs 10, 12 entre lesquels les flux sont transmis, ou des adresses (par exemple les numéros de téléphone) des utilisateurs des ordinateurs 10 et 12.

Le procédé de surveillance selon l'invention est mis en œuvre par un serveur de surveillance par lequel transitent les paquets SIP. Ce serveur de surveillance est généralement également dédié au traitement des paquets SIP.

Le procédé de surveillance selon l'invention est donc mis en œuvre par un des serveurs de traitement SIP 20, 22, et consiste à surveiller les messages SIP transmis en mode paquets par le réseau 18 entre le terminal émetteur 10 et le terminal récepteur 12.

Pour un canal SIP donné, on estime une valeur de débit  $D_m$  pour un paquet SIP émis sur ce canal SIP et on compare cette valeur de débit  $D_m$  à une valeur de débit maximal autorisé  $D_{max}$ . On autorise alors la transmission du paquet SIP uniquement si la valeur de débit  $D_m$  pour ce paquet SIP ne dépasse pas la valeur de débit maximal autorisé  $D_{max}$ .

Le débit maximal autorisé  $D_{max}$  pour un canal SIP donné est préalablement défini et communiqué par l'opérateur aux serveurs de surveillance SIP 20, 22 qui mettent en œuvre le procédé de surveillance. L'opérateur communique également la taille maximale autorisée  $T_{max}$  pour un paquet. Cette donnée est utile aux serveurs de surveillance SIP lorsqu'un nouveau canal SIP est créé, et que les serveurs n'ont pas reçu suffisamment de paquets SIP pour pouvoir calculer la valeur de débit  $D_m$  du nouveau paquet émis sur le nouveau canal SIP créé.

Les valeurs du débit maximal autorisé  $D_{max}$  et de la taille maximale autorisée  $T_{max}$  dépendent du canal des messages SIP, c'est à dire des terminaux s'échangeant les messages SIP. Certains utilisateurs peuvent par exemple avoir besoin d'un débit SIP maximal autorisé plus grand, notamment lorsqu'ils utilisent des données chiffrées, le chiffrement augmentant le nombre de données à transmettre.

Tous les serveurs de traitement SIP du réseau ne sont pas nécessairement des serveurs de surveillance SIP. Aussi, il faut s'assurer que parmi tous les serveurs de traitement par lesquels un paquet SIP transite, l'un au moins de ces serveurs de traitement SIP soit un serveur de surveillance SIP.

5           Par exemple, l'invention peut être mise en œuvre par un unique serveur de surveillance SIP en tant que premier serveur de traitement traversé par les paquets SIP. On peut alors utiliser dans les routeurs 14, 16 un dispositif logiciel comme un pare-feu, pour forcer l'acheminement des paquets SIP vers ce premier serveur de traitement SIP.

10           De façon alternative, l'invention peut être mise en œuvre par un serveur de surveillance SIP qui est l'un quelconque des serveurs de traitement SIP du réseau SIP. On définit alors des règles de routage assurant un transit systématique des paquets SIP par ce serveur de traitement SIP..

Le procédé de surveillance représenté sur la figure 2 comporte une première étape 30 de réception d'un paquet SIP par le serveur de surveillance SIP 20, 22.

15           Lors de l'étape 32 suivante, le serveur de surveillance SIP 20, 22 identifie le canal SIP relatif au paquet reçu. Cette identification est possible grâce aux adresses de l'émetteur et du récepteur du paquet SIP reçu.

20           Lors de l'étape de test 34 suivante, le serveur de surveillance SIP 20, 22 teste si le paquet SIP reçu est relatif à un canal SIP nouvellement créé ou à un canal SIP en cours d'utilisation.

25           Si le canal SIP est nouvellement créé, on passe à une étape 36 de création d'une liste nommée *Liste\_Derniers\_Paquets* qui garde en mémoire pour chaque canal SIP la taille et l'instant de réception de tous les paquets relatifs à ce canal SIP reçus depuis une durée D préalablement fixée par l'opérateur. La liste *Liste\_Derniers\_Paquets* fonctionne comme une fenêtre temporelle glissante : les informations relatives au dernier paquet reçu sont insérées à la liste alors que les informations relatives aux paquets reçus depuis plus longtemps que la durée D sortent de la liste. Les premiers paquets entrés dans la liste sont également les premiers sortis.

30           Lors de l'étape de test 38 suivante, le serveur de surveillance SIP vérifie si la taille T du paquet reçu est inférieure à la taille Tmax maximale autorisée pour un paquet.

Si la taille T du paquet reçu est inférieure à la taille Tmax autorisée, on passe à une étape 40 de transmission du paquet reçu par le serveur de surveillance SIP.

35           Sinon, on passe à une étape de test 42 lors de laquelle le serveur de surveillance teste si le paquet SIP reçu correspond à une requête SIP ou à une réponse SIP.

-7-

Si le paquet reçu correspond à une requête, on passe à une étape 44 au cours de laquelle le serveur de surveillance SIP 20, 22 ne transmet pas cette requête au destinataire mais la supprime et envoie une réponse d'erreur à l'émetteur du paquet.

5 Si le paquet reçu correspond à une réponse, on passe à une étape 46 lors de laquelle le serveur de surveillance SIP ne transmet pas la réponse au destinataire et envoie un message de type 'annulation' au destinataire.

10 Si lors de l'étape 34 le serveur de surveillance constate que le paquet reçu correspond à un canal SIP en cours d'utilisation on passe à une étape 48 de mise à jour de la liste *Liste\_Derniers\_Paquets* relative au canal SIP du paquet reçu. Cette mise à jour consiste à ajouter à cette liste les informations concernant le dernier paquet reçu et à supprimer de cette liste les informations concernant les paquets reçus depuis plus longtemps que la durée D de stockage.

15 Lors de l'étape 50 suivante, le serveur de surveillance SIP estime le débit moyen  $D_m$  des paquets relatifs au canal SIP du dernier paquet reçu. Ce débit moyen est estimé en divisant la somme des tailles des paquets stockées dans la liste *Liste\_Derniers\_Paquets* par la durée D de stockage.

Lors de l'étape de test 52 suivante, le serveur de surveillance SIP vérifie si le débit moyen  $D_m$  est inférieur au débit maximal autorisé  $D_{max}$ .

20 Si le débit moyen  $D_m$  est inférieur au débit maximal autorisé  $D_{max}$ , on passe à l'étape 40.

Si le débit moyen  $D_m$  est supérieur au débit maximal autorisé  $D_{max}$ , on passe à l'étape 42.

## REVENDEICATIONS

1. Procédé de surveillance de messages destinés à l'initialisation de sessions d'échange de flux multimédias, ces messages étant transmis en mode paquets via un serveur de surveillance (20, 22) par un réseau (18) entre un terminal émetteur (10) et au moins un terminal récepteur (12), caractérisé en ce qu'il comporte les étapes suivantes :

- on estime (50) une valeur de débit pour au moins un paquet d'initialisation reçu par le serveur de surveillance (20, 22),
- on compare (52) cette valeur à une valeur de débit maximal autorisé,
- on autorise (40) la transmission du paquet d'initialisation uniquement si la valeur de débit pour ce paquet d'initialisation ne dépasse pas la valeur de débit maximal autorisé.

2. Procédé de surveillance de messages transmis en mode paquets selon la revendication 1, dans lequel on définit pour chaque couple formé d'un terminal émetteur et d'un terminal récepteur, un canal de transmission, associé à une valeur de débit maximal autorisé spécifique.

3. Procédé de surveillance de messages transmis en mode paquets selon la revendication 1 ou 2, dans lequel l'estimation de la valeur de débit pour le paquet d'initialisation reçu par le serveur de surveillance comporte les étapes suivantes :

- on garde en mémoire les tailles des derniers paquets d'initialisation émis par le terminal émetteur (10) à destination du terminal récepteur (12) et reçus par le serveur (20, 22) de surveillance depuis une durée prédéterminée,
- on divise la somme des tailles des paquets d'initialisation mémorisés par la durée prédéterminée.

4. Procédé de surveillance de messages transmis en mode paquets selon l'une des revendications 1 à 3, mis en œuvre par le serveur de surveillance (20, 22), celui-ci étant en outre dédié au traitement des paquets d'initialisation de sessions.

5. Procédé de surveillance de messages selon la revendication 4, dans lequel on contraint l'acheminement des paquets d'initialisation de sessions vers le serveur de surveillance (20, 22) en tant que premier serveur de traitement traversé par ces paquets d'initialisation de sessions.

6. Procédé de surveillance de messages selon la revendication 4, dans lequel le serveur de surveillance (20, 22) étant l'un quelconque des serveurs de traitement des

paquets d'initialisation de sessions, on définit des règles de routage assurant un transit systématique des paquets d'initialisation de sessions par ce serveur de traitement.

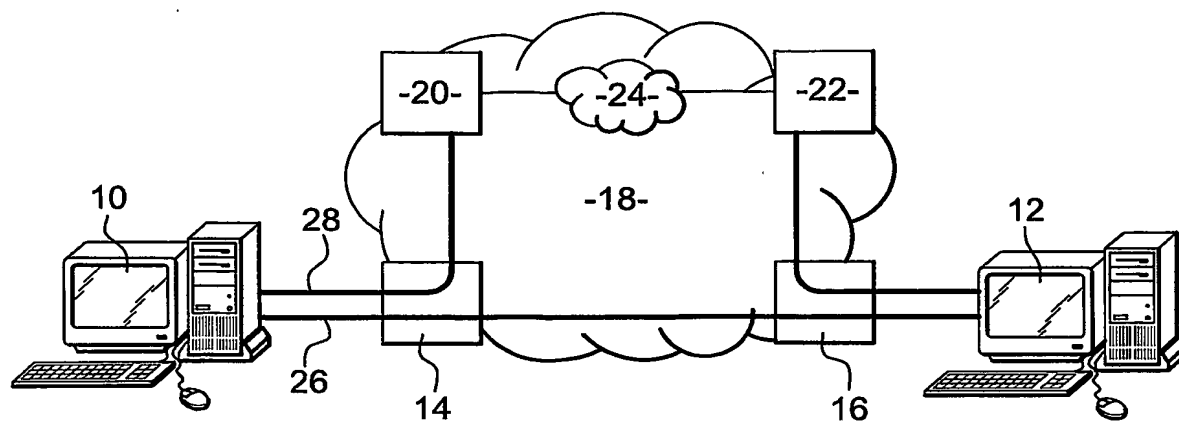
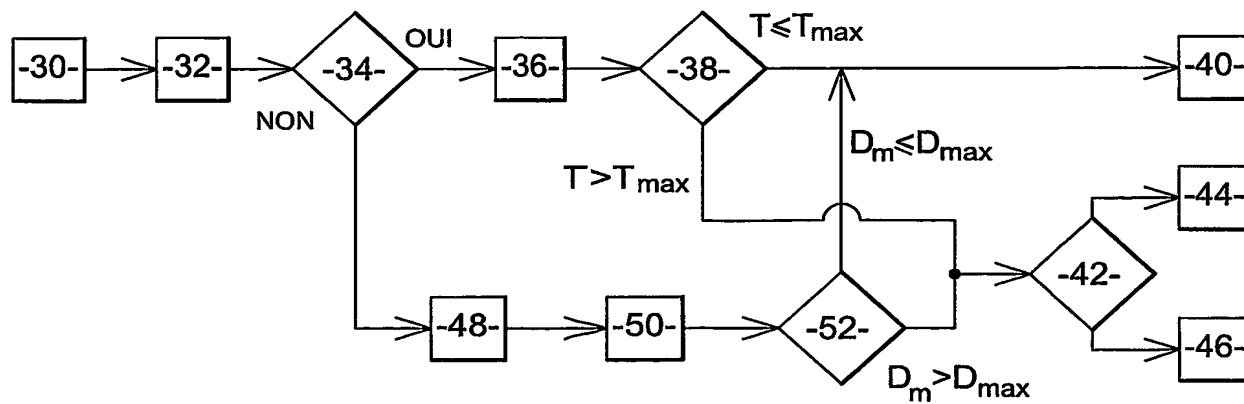
7. Procédé de surveillance de messages transmis en mode paquets selon l'une quelconque des revendication 1 à 6, dans lequel les messages d'initialisation de sessions transmis utilisent le protocole SIP.

8. Serveur (20, 22) de surveillance de messages destinés à l'initialisation de sessions d'échange de flux multimédias, ces messages étant transmis en mode paquets via un serveur de surveillance par un réseau (18) entre un terminal émetteur (10) et au moins un terminal récepteur (12), caractérisé en ce qu'il comporte :

- 10                   – des moyens d'estimation (50) d'une valeur de débit pour au moins un paquet d'initialisation reçu par le serveur de surveillance (20, 22),
- des moyens de comparaison (52) de cette valeur à une valeur de débit maximal autorisé,
- 15                   – des moyens d'autorisation (40) de la transmission du paquet d'initialisation uniquement si la valeur de débit pour ce paquet ne dépasse pas la valeur de débit maximal autorisé.

9. Installation de transmission de messages destinés à l'initialisation de sessions d'échange de flux multimédias comportant un réseau (18), comprenant au moins un serveur de surveillance (20, 22) selon la revendication 8.

1/1

**Fig. 1****Fig. 2**

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR2004/002680

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L29/06 H04L12/26

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	H. KHARTABIL: "Congestion safety and Content Indirection" 'Online! 2 September 2003 (2003-09-02), pages 1-20, XP002286171 Retrieved from the Internet: URL: <a href="http://www.ietf.org/internet-drafts/draft-khartabil-sip-congestionsafe-ci-02.txt">http://www.ietf.org/internet-drafts/draft-khartabil-sip-congestionsafe-ci-02.txt</a> > 'retrieved on 2004-06-28! page 3, paragraph 2.0 page 8, paragraph 5.2 page 10, paragraph 5.3 page 13, paragraph 8.0 ----- -/--	1,2,4-9

☒ Further documents are listed in the continuation of box C.☐ Patent family members are listed in annex.

## ° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&amp;" document member of the same patent family

Date of the actual completion of the international search

27 January 2005

Date of mailing of the international search report

04/02/2005

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Mannekens, J

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/FR2004/002680

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>D. WILLIS, B. CAMPBELL: "Session Initiation Protocol Extensions to Assure Congestion Safety" 'Online! 13 August 2003 (2003-08-13), pages 1-13, XP002286172 Retrieved from the Internet: URL: <a href="http://www.ietf.org/internet-drafts/draft-ietf-congestsafe-01.txt">http://www.ietf.org/internet-drafts/draft-ietf-congestsafe-01.txt</a> 'retrieved on 2004-06-28! the whole document</p> <p>-----</p>	1-9

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR2004/002680

**A. CLASSEMENT DE L'OBJET DE LA DEMANDE**  
CIB 7 H04L29/06 H04L12/26

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

**B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE**

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data, PAJ

**C. DOCUMENTS CONSIDERES COMME PERTINENTS**

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	<p>H. KHARTABIL: "Congestion safety and Content Indirection" 'Online! 2 septembre 2003 (2003-09-02), pages 1-20, XP002286171 Extrait de l'Internet: URL: <a href="http://www.ietf.org/internet-drafts/draft-khartabil-sip-congestionsafe-ci-02.txt">http://www.ietf.org/internet-drafts/draft-khartabil-sip-congestionsafe-ci-02.txt</a> &gt; 'extrait le 2004-06-28! page 3, alinéa 2.0 page 8, alinéa 5.2 page 10, alinéa 5.3 page 13, alinéa 8.0</p> <p style="text-align: center;">----- -/--</p>	1, 2, 4-9

☒ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

\* Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

27 janvier 2005

Date d'expédition du présent rapport de recherche internationale

04/02/2005

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Mannekens, J

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	<p>D. WILLIS, B. CAMPBELL: "Session Initiation Protocol Extensions to Assure Congestion Safety" 'Online! 13 août 2003 (2003-08-13), pages 1-13, XP002286172</p> <p>Extrait de l'Internet:  URL:http://www.ietf.org/internet-drafts/draft-ietf-congestsafe-01.txt&gt;  'extrait le 2004-06-28!  le document en entier</p> <p style="text-align: center;">-----</p>	1-9